CURSO DE ESTRATEGIAS DE DEFENSA EN CIBERSEGURIDAD

1. Temática principal del curso

Las estrategias de defensa en ciberseguridad fijan como uno de sus principales objetivos garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de las capacidades de prevención, defensa, detección, análisis e investigación de los ciberataques.
La acción formativa Estrategias de Defensa en Ciberseguridad trata de forma técnica y práctica los aspectos tecnológicos más relevantes en la protección de aplicaciones, sistemas, infraestructura, redes de control y automatización industrial en dos fases:

- En una primera fase se abordan los principales riesgos de seguridad que afectan a estas infraestructuras, tanto desde el interior como desde el exterior de las organizaciones. Se profundiza en el estudio de las principales vulnerabilidades a nivel de protocolos de control y automatización, de las arquitecturas de redes y sistemas, gestión y operación, así como en su diseño e implementación.
- La segunda fase de la formación aborda las distintas estrategias y requisitos de seguridad para el desarrollo e implantación de aplicaciones y sistemas de automatización y control industrial seguros teniendo en cuenta las buenas prácticas de ciberseguridad industrial, así como las distintas tecnologías de prevención, monitorización y protección específicamente diseñadas para estos entornos.

2. Objetivos del curso

1. Conocer las amenazas, riesgos y vulnerabilidades relacionadas al uso de las nuevas tecnologías.
2. Conocer y aplicar buenas prácticas de ciberseguridad para la prevención de riesgos digitales.
3. Comprender y configurar las medidas de seguridad adecuadas para proteger nuestros dispositivos de trabajo y comunicación: ordenador, tablet, smartphone,…
4. Conocer y aplicar técnicas de seguridad para garantizar la confidencialidad e integridad de la información privilegiada que utilizamos.
5. Diseñar, configurar y aplicar estrategias de defensa para la seguridad perimetral en la red corporativa.
6. Conocer y aplicar técnicas de desarrollo seguro para prevenir vulnerabilidades en las aplicaciones.
7. Desarrollar y aplicar un Sistema de Gestión de la Seguridad de la Información.

3. Fechas y horarios

El curso constará de 260 horas lectivas así como de otras 60 horas iniciales de Desarrollo de Habilidades Personales.

El curso se impartirá en las siguientes fechas: 20/11/2017-23/02/2018

Con un horario de mañana de: 8:00-14:00

4. Temario

- Aproximación a la Empresa: Desarrollo de Habilidades Personales para la Empleabilidad.
    - Acercamiento a las temáticas de la acción formativa a cursar. (20h)
    - Dinámicas de trabajo en motivación, aprendizaje, trabajo en equipo e inteligencia emocional. (40h)
- Ciberseguridad, conceptos y estrategias generales de defensa. (15h)
- Concienciación en seguridad, guía de buenas prácticas. (15h)
- Medidas, técnicas y utilidades para la protección de sistemas y dispositivos finales. (50H)
- Seguridad de la información, estrategias y técnicas para la protección de información sensible. (70h)
- Arquitectura de seguridad perimetral y corporativa. (40h)
- Técnicas de desarrollo seguro de aplicaciones. (45h)
- Implementación de una estrategia de Gestión y Gobierno de la Seguridad. (25h)

5. Lugar de impartición

Madrid.

SAREKO SEGURTASUNEKO DEFENTSA ESTRATEGIAK

1. Ikastaroaren gai nagusiak

Sareko Segurtasuneko Defentsa Estrategien helburu nagusiena sareen eta sistema informatikoen erabilera segurua bermatzea da. Horretarako, prebentzio, defentsa, hautemate eta analisi gaitasunak indartzea oso garrantzitsua da.

- ESareko Segurtasuneko Defentsa Estrategien ikastaroak aspektu teknologiko aipagarrienak – aplikazioak, sistemak, azpiegiturak, kontrol sareak eta automatizazio industriala– modu teoriko eta praktikoan lantzen ditu bi faseetan:

- Lehenengo fasean azpiegitura hauei eragiten dieten arriskuak lantzen dira, kanpokoak nahiz barnekoak. Sare eta sistemen antolaketan sakontzen da eta baita bere diseinu eta inplementazioan.

  Bigarren faseak segurtasun estrategia eta baldintza ezberdinak lantzen ditu. Sareko segurtasun industrialaren praktika egokiak kontuan hartuz, aplikazio eta sistemen automatizazioan oinarrituz. Prebentzio teknologia desberdinak, monitorizazioa eta horrelako inguruetarako diseinatutako babesa ere lantzen dira.

2. Ikastaroaren helburuak

1. Teknologia berrien erabilerari lotutako mehatxuak, arriskuak eta zaurgarritasunak ezagutzea
2. Arrisku digitalei aurrea hartzeko, sareko segurtasuneko praktika egokiak ezagutu eta aplikatzea.
3. Segurtasun neurri egokiak ulertu eta konfiguratu gure laneko eta komunikazioko gailuak babesteko: ordenagailuak, mugikorrak…
4. Segurtasun teknikak ezagutu eta erabiltzea maneiatzen dugun informazio pribilegiatuaren osotasuna eta konfidentzialtasuna bermatzeko

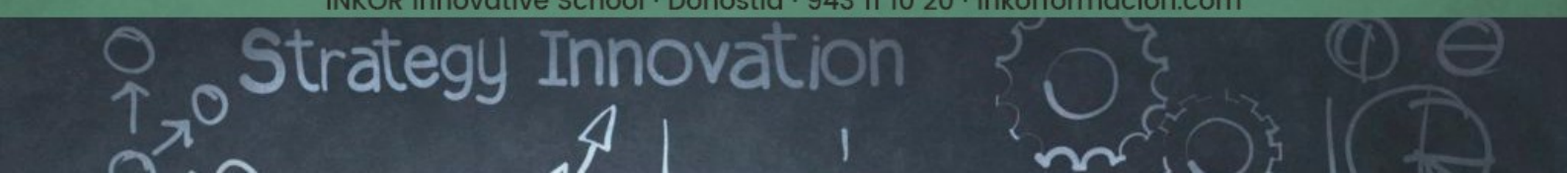
   Inguruko segurtasuneko sare korporatiborako defentsa estrategiak diseinatu, konfiguratu eta erabiltzea.

5. Inguruko segurtasuneko sare korporatiborako defentsa estrategiak diseinatu, konfiguratu eta erabiltzea.
6. Aplikazioetako zaurtasunei aurrea hartzeko garapen seguruaren teknikak ezagutu eta erabiltzea.
7. Informazioaren Kudeaketa Sistema bat garatu eta erabiltzea

3. Datak eta ordutegiak

Ikastaroak 260 eskola-ordu izango ditu eta beste 60 haste-ordu trebetasun pertsonalen garapenerako. Ikastaroa ondorengo egunetan izango da:

2017/11/20 - 2018/02/23 goizeko ordutegiarekin: 8:00-14:00



4. Edukiak

- Enpresa hurbilketa: Enplegu ahalmenerako trebetasun pertsonalen garapena (60 ordu)
    - Ikasi beharreko gaien hurbiltzea
    - Lan dinamikak motibazioan, ikaskuntzan, talde lanean eta adimen emozionalean.
- Sareko segurtasuna, kontzeptuak eta defentsa estrategia orokorrak (15 ordu)
- Segurtasunaren kontzientziazioa, praktika egokien gida (15 ordu)
- Sistema eta gailuen babeserako neurriak, teknikak eta erabilgarritasunak (50 ordu)
- Informazioaren segurtasuna, estrategiak eta informazio sentikorraren babeserako teknikak (70 ordu).
- Aplikazio seguruen garapenerako teknikak (45 ordu)
- Segurtasun Gobernu eta Kudeaketa estrategia baten inplementazioa (25 ordu)

  Implementación de una estrategia de Gestión y Gobierno de la Seguridad.

5. Lugar de impartición

Madrid.